Attachment E

Operations Branch Service Level Agreement for Systems Administration Services

Objective

Document and establish the support services associated with the Systems Administration and management of TIER II/III systems support

Service Description

NDU-ITD-OPSD provides centrally managed hosting solutions for the applications required to meet the mission of the National Defense University (NDU). Through the use of advanced technology, ITD provides multiple platforms geared to meet customers' computing needs. This service provides customers with a reliable, monitored, secure, and managed solution with the flexibility and performance of distributed computing solutions.

This distributed hosting service design includes multiple, redundant, and diverse high-speed Internet connections, security systems and procedures, cooling and environmental systems, and redundant power. Business continuity is a requirement by establishing and maintaining off-site data storage and recovery in a fully staffed and environmentally sound facility.

HRC offers distributed computing solutions on multiple platforms; primarily Windows Server and Desktop and Apple based systems. ITD provides installation, upgrades and monitoring support for the infrastructure and software.

ITD offers a wide variety of storage capabilities including tape and disk. ITD provides several levels of disk and tape storage including mid-range disk storage, Network Addressable Storage (NAS) devices (Future), Serial Advanced Technology Attachment (SATA) and Fibre Channel disk systems, and Storage Area Network (SAN) attached storage.

ITD's distributed offerings also come with standard reporting capabilities that provide utilization, performance and trending information.

Catalog of Services

The following services are included:

- Tape Backup / Recovery
    - Standard tape rotation / retention schedule

  - Daily incremental backups – retained off-site for 14 days
  - All daily and weekly tapes are moved off-site daily for vault storage
  - Standard daily backups.

- Hardware support and maintenance
  - ITD's systems administrators install and set up all server hardware in accordance with industry and DoD requirement and best practices. Also, in conjunction with the hardware OS vendors, ITD's systems administrators will apply firmware patches to systems to ensure full compliance with DoD, Army and ITD standards and policies.
  - ITD will also repair or replace any hardware component shown to be detrimental to the continued operation of a system

- Operating system (OS) support and maintenance
  - ITD Systems Administrators, in conjunction with the Information Assurance Office and OS Vendors, will apply patches to operating systems in accordance with DoD, Army and ITD standards and policies.

- Capacity, performance and system monitoring
  - ITD monitors several key items for all servers
  - Standard monitoring features included::
    - Utilizing available monitoring tools for the network, server and storage environment.
    - The following monitoring modules will be the baseline default to be loaded on each server to monitor the applicable pieces of the operating system:
      - File System (Monitored for warning and alarm levels) / Logical File System (Windows)*
      - Memory
      - Kernel
      - CPU (Monitored for warning and alarm levels) / NT_CPU (Windows)*
      - Processes (Monitored as requested)
      - Log files (Monitored as requested)
      - SWAP File (Monitored for UNIX Systems – Summary)*
      - Health at a Glance (Monitored for Windows Systems - memory usage)*
      - Event Management – Alerts / Management
  - Server Farm / Network Infrastructure Monitoring
    - Standard fault, configuration, performance and security management monitoring, including:
      - Fault detection with notification to operational personnel

        - Collecting and reporting on performance metrics
        - Device authentication, authorization and accounting

* email and pager alerts will be sent (email for warning and email and pager for alarm)

- **Customer services**

  ITD Systems Administrator Team Leads are responsible for obtaining customer requests for Systems Administration services and performing needs assessments. Upon completion of the needs assessment, the Systems Administrator Team Lead will put together a project team and create an implementation plan. The Systems Administrator Team Lead will assist the customer, when needed, on interactive project management, ensuring that the project is kept on schedule and providing escalation when required. The Systems Administrator Team Lead will prepare server configurations to meet business requirements and will provide cost proposals. The Systems Administrator Team Lead also supports the generation of Purchase Order (PO) requisitions and coordinates with hardware and software vendors for delivery of equipment.

Hours of Availability

Service is available to customers 0600 – 1800, Monday - Friday, excluding planned outage maintenance windows and unavoidable events. Maintenance windows are used only when needed for planned changes that have gone through the ITD Change Management Process. In addition to the Standard ITD Maintenance Windows, site-specific changes may be coordinated with customers at non-standard times.

Standard maintenance windows are defined as:

- 1800 to 0200 each Wednesday

Services supported by ITD Systems Administration staff include the following:

- Initial server purchase
    - Business requirements analysis, configurations and cost proposal analysis with the customer
    - Security analysis
    - Setup of all components
    - Installation of the server, OS and monitoring tools
    - Hosting, monitoring, backup, security scans, and support
    - Life cycle hardware upgrades (typically 3 - 5 year cycle) required by a customer (additional processors, memory, etc.)

Customer Service Support

- Hours of Support (0600 – 1800, Monday – Friday)

  The ITD Customer Service Section is responsible for the support of the Tier I Information Technology (IT) infrastructure. System monitoring is provided via alerts generated from monitoring software and a notification (pager/email) to the on-call Systems Administrator. The Operations Branch Administrators are responsible for providing business and technical infrastructure analysis, problem solving, and first and second level diagnostics.

  - Call the ITD Help Desk or Operations Center at 202-685-3724

- Incidents and Service Requests

  - Ticket Creation

    Any critical Incident should be initiated by opening a Service Request ticket. If the Incident is of a critical nature then it is vital that this ticket receives proper prioritization.

  - Prioritization

    The ITD Help assigns a Priority to every Incident or Service Request that is initiated. The Prioritization Model is used to ensure a consistent approach to defining the sequence in which an item needs to be resolved and to drive the assignment of resources.

    The Priority depends upon:
    - The Impact on the business: size, scope and complexity of the Incident
    - The Urgency to the business: time within which resolution is required
    - The resource availability
    - The expected effort in resolving or completing a task
    - Incident Target Customer Status Update and Resolution Times

      The following chart shows the Incident Target Customer Status Update and Target Resolution Times by Priority after creation and initial assessment / assignment of a ticket by the Help Desk or Operations Center. Resolution Times are measured in clock hours and/or minutes unless otherwise specified.

- The Target Resolution Time is the total time from ticket creation to Incident resolution and restoration of service to the user. Service may be restored either by a workaround or by a permanent solution. ITD strives to resolve ninety percent of Incidents within the time frame specified for each Priority.

Priority	Target Customer Status Update Time	Target Resolution Time
Critical	Every 60 minutes or as agreed upon with the Customer(s)	4 hours or less
High	Every 2 hours or as agreed upon with the Customer(s)	8 hours or less
Medium	Upon request	24 hours or less
Low	Upon request	3 business days

Customer Notification

ITD-OPSD will provide periodic updates to the customers and management as Incidents are being worked and upon Incident resolution. ITD will also provide communications when Incidents or outages occur that may impact the customer. In addition, ITD will notify customers of upcoming change events that may have the potential to impact supported ITD services and lines of business.

HRC will communicate via ticket updates, phone calls, and/or email notifications utilizing the customer contact information. Customers are responsible for providing the ITD Help Desk or Operations Center with current contact information.

Change Management

By following the ITIL-Based Change Management Process, ITD strives to minimize the business impact of changes on ITD customers and to maximize the stability of ITD environment by following a clearly defined process and by complying with ITD policies. ITD will notify customers of upcoming change events that may have the potential to impact supported ITD services and lines of business. Customers should provide a list of customer contact names to the ITD Help Desk or Operations Center for notification purposes.

If an Incident results in a Request for Change (RFC) generated,, the Operations Branch policy for lead time will be followed based upon wherever it is feasible. The three levels of change types are Major, Significant and Minor. A Major Change requires a minimum of 14 business days lead time. If the RFC will or could have global customer impact and/or require substantial financial/ ITD resource commitment, or customer impact, it is identified as a Major Change. A Significant Change requires a minimum of 5 business days lead time. If the RFC will or could have localized and substantial, financial, ITD resource commitment, or customer impact, it is identified as a Significant Change. A Minor Change requires 1 business days lead time and has little or no impact.

Customer Changes

Using the defined lead times above, the Customer will provide a forward schedule of change to the ITD Help Desk or Operations Center of any customer (or vendor) event affecting the Customer's system. The need for notification arises in situations that include, but are not limited to, modifications to code, configuration of systems, access requirements outside of the existing SLA, or any need the Customer may have for additional ITD resources, either IT or personnel. The notification requirements are especially important for events that could affect shared services, system monitoring status or resource usage, such as storage or server utilization. The ITD Help Desk or Operations Center will coordinate any communications among ITD and customers to minimize the impact of these events.

Urgent Changes

At times unplanned events occur resulting in an impact to systems. The ITD Change Management Process accounts for these situations. Such an event may require an Urgent Change. An Urgent Change could be related to an IT component failure, regulatory event, or an event driven by an emergency such as severe weather. In all cases, an unforeseen event is considered an urgent event and will be handled with as much communication as possible and as soon as possible. Customers and ITD personnel are responsible for notifying the Service Desk of such events. The Service Desk is responsible for all communications for events of this nature.

Security Standards and Policies

- ITD services adhere to the Department of Defense (DoD), Army, and ITD Security Standards and Policies
- The Customer is responsible for ensuring that their systems and services are compliant with and follow Department of Defense (DoD), Army, and ITD Security Standards and Policies

Business Continuity Plan

ITD has a Continuity of Operations Plan (COOP) to ensure the continuity of critical business functions.

Customer Responsibilities

- Contact the ITD Help Desk or Operation Center:
    - When modifications are being applied to applications
    - When changes are slated to be applied to ensure overlapping maintenance changes do not occur
    - If the installation of an OS or security patch is known to have an adverse impact on a customer application(s). The customer shall assume all risk associated with not installing the patch.
- Provide a list of approved customer contacts who can request changes to the application environment to the ITD Service Desk. This list should include contacts for both standard business hours and, if applicable, 24 X 7 supports.
- Determine amount of storage needed to minimize costs
- Plan ahead to ensure that required storage is available as needed

Systems Administrator Responsibilities

- Installation of Tier I and Tier II systems software
- Maintenance of systems software to include testing and patching
- Inventorying and providing status update on systems software releases
- The development of required functionality that is not provided in the basic “off-the-shelf” (COTS) products
- The application of program fixes for software provided by Government contracted vendors or for software developed in-house
- The resolution of system problems
- The development of computer operating standards and procedures
- The management of the configuration and change management process
- Computer Performance and Capacity management

Level of Support: Windows 2003 (Intel)

Branch	SERVICE/SUPPORT PROVIDED

OPSD	Systems Administration Windows 2003 / 2008 Server VMWare
Service	Definition and Description
Systems Administration (Windows 2003)	Provide system administration and operating system support for Windows Operating environment and Windows Applications. System Availability: TBD (Maintenance Window as Required) Problem Response Time: 2 hours. Reliability: 99.5% uptime Normal Duty Hours: M – F 0600 - 1730 Backup Schedule: Full System – Daily
Systems Administration (Windows 2003)	Provide Continuity of Operations Support (COOP) Availability: M - Sa Offsite Frequency: Daily (M – Sa) Recovery Point Objective: 24 hours Recovery Time Objective: 24 – 36 hours (Critical Systems)
Systems Administration (Monitoring)	Monitor system logs, security logs, and application logs - Performed 24 x 7 x 365 (Excluding System Unavailability)
Systems Administration (Security)	Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration Windows 2003 / 2008 Server VMWare
Service	Definition and Description
Non Specific Services	• Installing new servers • Performing network configuration • System account management • Monitoring file system and disk usage • Monitoring system availability • Periodic testing of recovery procedures • Applying system and application patches • Monitoring for suspicious system activity • Installing commercial software (as per license agreement) • Installing supported public-domain software

Level of Support: Enterprise Storage Systems

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration EMC Clariion NetApp Applework (being decommissioned) Brocade Fibre Channel Switches Total Storage Capacity – 225 Terabytes
Service	Definition and Description
Systems Administration (Enterprise Storage Systems)	Provide system administration and operating system support the storage infrastructure to include provisioning and capacity management. System Availability: 24x7x365 (Maintenance Window as Required) Problem Response Time: 2 hours. Reliability: 99.5% uptime Normal Duty Hours: M – F 0600 - 1730

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration EMC Clariion NetApp Applework (being decommissioned) Brocade Fibre Channel Switches Total Storage Capacity – 225 Terabytes

Service	Definition and Description
Systems Administration (Enterprise Storage Systems)	Support Storage Allocation/Reconfiguration requests Availability: 24x7x365 Normal Duty Hours: M – F 0630 - 1730
Systems Administration (Monitoring)	Monitor system logs and event logs - Performed 24 x 7 x 365 (Excluding System Unavailability) (Automated)
Systems Administration (Security)	Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Level of Support: Open Systems Backup Recovery

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration HP Tape Library LTO- 4 Tape Drives Symantec Netbackup Software

Service	Definition and Description

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration HP Tape Library LTO- 4 Tape Drives Symantec Netbackup Software

Service	Definition and Description
Systems Administration (Backup/Recovery)	Provide system administration and Business Continuity Management and support for the Open Systems Backup Recovery environment. • Provides backup/recovery of all Open Systems files on a daily basis. • Supports the ITD COOP in both the execution of the recovery of the Open Systems environment and the validation of procedures and their effectiveness. System Availability: 24x7x365 (Maintenance Window as Required) Problem Response Time: 2 hours. Reliability: 99.5% uptime Normal Duty Hours: M – F 0600 - 1730
Systems Administration (Backup/Recovery)	Support Request for Data Recovery Availability: M – F (Excluding emergencies) Normal Duty Hours: M – F 0630 – 1730 (In the event of an emergency, Backup Administrator will respond within 2 hours to initiate recovery request)
Systems Administration (Monitoring)	Monitor system logs and event logs - Performed 24 x 7 x 365 (Excluding System Unavailability) (Automated)

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration HP Tape Library LTO- 4 Tape Drives Symantec Netbackup Software
Service	Definition and Description
Systems Administration (Security)	Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Level of Support: Monitoring

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration What's Up Gold SCCM SCOM CiscoWorks Unisphere
Service	Definition and Description

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration What’s Up Gold SCCM SCOM CiscoWorks Unisphere

Service	Definition and Description
Systems Administration	Performance monitoring and reporting to include applications response and resource utilization, and general performance statistics server. Performance monitoring and reporting on network, storage and server environments Installation and customization of performance management and reporting tools. • Using centralized performance management and capacity planning tools, provide evaluation of overall system performance by compiling real-time and historical system information of the server / network environment within ITD. • Generates alerts to notify the respective Systems Administrator of potential problems with a given server. System Availability: 24 x 7x 365 (Maintenance Window as Required) Problem Response Time: 2 hours. Benefits • Cross platform integration • Centralized job management • Access control restriction
Systems Administration	Monitor system logs and event logs - Performed 24 x 7 x 365 (Excluding System Unavailability) (Automated)

Level of Support: SQL Server Administration / Enterprise Application

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration SQL Server

Service	Definition and Description
Systems Administration	Installation, maintenance, and management of system software. Ensuring that backup and recovery measure are in place to safeguard data as prescribed in the agreement with the customer. Provides system technical support, enhancements, upgrades via coordination with customer or vendor. Identifies data recoverability requirements based on the risk to the business • The maintenance of systems software to include the installation and testing of various operating systems releases and patches. • The development of customized program interfaces to provide a required functionality that is not provided in the basic “off-the-shelf” software products. • The application of program fixes for software acquired from Government contracted vendors or for software developed in-house. • Participates in the resolution of system problems. • The application of software security patches, fixes, and DISA security configuration guidelines to maintain Information Assurance, IAVA, and accreditation objectives. • • Support COOP through the re-creation of the Application / Database Environments. System Availability: Based on the needs of the customer Problem Response Time: Based on the needs of the customer
Systems Administration	Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Level of Support: Web Administration

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration Apache IIS SSL Capabilities

Service	Definition and Description
Systems Administration	Infrastructure support for the underlying web architectural environment for the development, test, and production environments. System Availability: Based on the needs of the customer Problem Response Time: Based on the needs of the customer
Systems Administration	Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Level of Support: Exchange

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration Exchange 2010

Service	Definition and Description
Systems Administration	Administer the Enterprise eMail solution providing mail services and storage System Availability: 24 x 7 x 365 Problem Response Time: Based on the needs of the customer

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Systems Administration Exchange 2010

Service	Definition and Description
Systems Administration (Security)	Administer the Blackberry Enterprise Service. Troubleshoot blackberry handheld devices. Administer the Outlook Web Access Service. Provide support to the NEIS by supporting the domain, server, and desktop configurations. Perform Exchange backups. Administer and develop Remedy services to include Help Desk, and Change Tasking (configuration management). Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Level of Support: Domain Administration

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Domain Administration
Service	Definition and Description
Systems Administration	Provide Domain Service Administration System Availability: 24x7x365 Problem Response Time: 2 hours
Systems Administration	• Administer the McAfee Host Based System Security (HBSS) Program ensuring that desktops and elements within the infrastructure are properly configured, and remain up to date based on the latest security requirement • Administer the Workstation Software Update Services (WSUS / SCCM) Enterprise Program ensuring that desktops are properly configured, and remain up to date with the latest Microsoft patches and hotfixes. • Administer the File and Print Services Enterprise solution offering central file storage with the ability to share files. • Provide Enterprise Desktop Authority Scripting Service allowing for file share, and printing services, and en masse desktop changes that are required to respond to an enterprise issue or vulnerability. Allows for en masse broadcasting. • Administer the Systems Management Server enterprise solution. Focus on software delivery, discovery services, Remote Control. • Administer the SCOM solution. Focus on server administration, logging. • Create standard enterprise core desktop image. • Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Level of Support: Network Management

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Network Management Provide support to the NEIS network architecture, including, network applications, and network communication devices and capabilities. Perform the installation and configuration of hardware and software items, including, but is not limited desktops, servers, wiring from the desktop through network communications devices to wire management panels, network communications devices, router, and switch connection installations, both internally (NOC) and to the WAN. Monitors network operations and performance ensuring system/network availability and throughput. Continually adjusts system parameters, tuning system performance, optimizing processing speed and capabilities. Ensures the networks, systems, and databases are secured from unauthorized users and programs by firewall and antivirus software.
Service	Definition and Description
Systems Administration	Network Management System Availability: 24x7x365 Problem Response Time: 2 hours

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Network Management Provide support to the NEIS network architecture, including, network applications, and network communication devices and capabilities. Perform the installation and configuration of hardware and software items, including, but is not limited desktops, servers, wiring from the desktop through network communications devices to wire management panels, network communications devices, router, and switch connection installations, both internally (NOC) and to the WAN. Monitors network operations and performance ensuring system/network availability and throughput. Continually adjusts system parameters, tuning system performance, optimizing processing speed and capabilities. Ensures the networks, systems, and databases are secured from unauthorized users and programs by firewall and antivirus software.

Service	Definition and Description
Systems Administration	• Review and assess the network information architecture to ensure that it is compliant with industry and DoD best practices. Perform analytical reviews of information management programs supporting telecommunications for the NDU community. Recommend improvements on the use/allocation of resources at the least cost with the greatest efficiency. • Ensure the telecommunications network remains in an operational status. Engineer and supervise management of the telecommunications network. Prepare written and oral reports for higher level management of state-of-the-art data-communications software, hardware, and firmware systems. • Apply in-depth, technical knowledge of communications, ADP, security, technology, equipment and procedures ensuring the installation and operation of the data communications network meets the established requirements. In conjunction with engineering and managing the networking environment consider telecommunications technological trends; customer requirements; cost factors; and resource utilization trends in the development of planning guidance for the NDU community. • Develop, publish, apply and monitor policies, procedures and management practices to maintain and effectively use distributed capabilities. • Provide support and management of mobile equipment. • Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch.

Level of Support: Customer Service – Help Desk

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Customer Service Help Desk Support for operating systems, printers, scanners, plotters, PC's, wiring, network connectivity issues and Cot/Got off-the-shelf software installation and configuration. Responsible for creating deployable images of desktop personal computers, maintaining baseline images and re-imaging customer workstations. Required to open, update and close all customer support call into a trouble ticket and problem resolution database within the prescribed timeframe based upon the complexity of issue. Provide direct customer support and assistance to the NDU Community, including students, staff and faculty with issues ranging from, but not limited to, remote connectivity, laptop configurations, email, IT hardware and software, and internet access and other connectivity problems..
Service	Definition and Description
Systems Administration	• Develop, publish, maintain, and enforce the NEIS end-user standard/preferred software product list and standards for end-user Information Management (IM) equipment and related capabilities. • Manage the reutilization and redistribution of equipment (Tier III terminals, printers, desktops / laptops. • Manage end-user maintenance. Provide first call support prior to contract maintenance. • Maintain a maintenance shop with proper test equipment and tools to install equipment and diagnose end-user problems. • Perform equipment supply management to ensure that adequate replacement items in place to perform onsite repairs to end-user problems, analyze end-user equipment requirements, and solve problems relating to end-user hardware and software.

Branch	SERVICE/SUPPORT PROVIDED
OPSD	Customer Service Help Desk Support for operating systems, printers, scanners, plotters, PC’s, wiring, network connectivity issues and Cot/Got off-the-shelf software installation and configuration. Responsible for creating deployable images of desktop personal computers, maintaining baseline images and re-imaging customer workstations. Required to open, update and close all customer support call into a trouble ticket and problem resolution database within the prescribed timeframe based upon the complexity of issue. Provide direct customer support and assistance to the NDU Community, including students, staff and faculty with issues ranging from, but not limited to, remote connectivity, laptop configurations, email, IT hardware and software, and internet access and other connectivity problems..

Service	Definition and Description
Systems Administration (Security)	Install security Information Assurance Vulnerability Alert (IAVA) patches on all servers and test and verify system is not adversely affected by patch. - Within the suspense time/date provided in the applicable IAVA

Additional supported systems are included in the attachments.